PASCAL Journal of Computer Science and Informatics
https://jurnal.devitara.or.id/index.php/komputer
E-ISSN: 3047-5074 Volume 3 Nomor 2 Tahun 2026

A Comparative Analysis of the Efficiency of Blockchain Consensus Algorithms: Proof of Work, Proof of Stake, Delegated Proof of Stake, and Practical Byzantine Fault Tolerance

[1]Desman Karya Jaya Zega, [2]Laurensius So Putra Jaya Halawa, [3]Siaman Lase, [4]Melissa Putri Hutabarat
[1, 2, 3, 4] Informatics Study Program, Universitas Budi Darma, Medan, North Sumatra, Indonesia

ARTICLE INFO

Keywords:
Blockchain;
Consensus Algorithm;
Proof of Work;
Proof of Stake;
Delegated Proof of Stake;
Practical Byzantine Fault Tolerance.

Email :
desmanzega86@gmail.com

ABSTRACT

The rapid development of blockchain technology has accelerated the adoption of distributed systems across various sectors, including financial services, supply chain management, the Internet of Things (IoT), and digital government. Consensus algorithms play a fundamental role in blockchain by ensuring transaction validity and data consistency without relying on a centralized authority. Since each consensus mechanism exhibits different characteristics, a comparative analysis is required to identify its strengths and limitations. This study aims to analyze and compare the efficiency of four major blockchain consensus algorithms, namely Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT). The research employed a comparative literature study by collecting, selecting, and analyzing relevant scientific publications. The comparison was conducted based on transaction throughput, energy efficiency, communication complexity, transaction finality, network characteristics, and fault tolerance. The results indicate that no single consensus algorithm provides optimal performance across all evaluation parameters. PoW offers high security and decentralization but suffers from high energy consumption and low throughput. PoS provides a balanced trade-off among energy efficiency, security, and scalability, while DPoS improves transaction capacity through a delegated validator mechanism. PBFT achieves high throughput and instant transaction finality but is more suitable for permissioned blockchain environments with a limited number of participating nodes. This study proposes a comparative analysis framework that can serve as a reference for selecting an appropriate consensus algorithm based on blockchain implementation requirements.

INTRODUCTION

The rapid advancement of blockchain technology has significantly transformed the development of distributed information systems. Unlike conventional systems that rely on centralized authorities, blockchain enables every node within the network to maintain an identical copy of the distributed ledger and participate collectively in the transaction validation process. This decentralized architecture enhances transparency, data integrity, and fault tolerance, making blockchain an attractive solution for various application domains, including digital financial services, supply chain management, the Internet of Things (IoT), healthcare, and e-government (Nakamoto, 2008; Feng, 2025).

The effectiveness of blockchain implementation is largely determined by the consensus mechanism employed. Consensus algorithms enable distributed nodes to reach agreement on the validity of transactions without relying on a trusted third party. Over the past decade, numerous consensus mechanisms have been proposed to address different performance and security requirements, among which Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT) are the most widely adopted. Each algorithm exhibits distinct characteristics, offering specific advantages while also presenting limitations that influence the overall efficiency, security, and scalability of blockchain systems (Castro & Liskov, 1999; Li et al., 2017).

One of the most significant challenges in blockchain development is selecting a consensus algorithm capable of balancing the three fundamental properties of blockchain systems, namely security, decentralization, and scalability, commonly referred to as the Blockchain Trilemma. Proof of Work provides a high level of security through computational mining but suffers from excessive energy consumption and

relatively low transaction throughput. In contrast, Proof of Stake replaces computational mining with a staking mechanism, substantially reducing energy consumption while improving transaction processing capacity. Delegated Proof of Stake further enhances scalability by introducing a delegated validator mechanism, enabling faster transaction confirmation. Meanwhile, Practical Byzantine Fault Tolerance achieves deterministic transaction finality with minimal confirmation delay, making it particularly suitable for permissioned blockchain environments with a limited number of participating nodes (Saad et al., 2021; Shen et al., 2025).

Numerous studies have investigated the performance of blockchain consensus algorithms from different perspectives. Li et al. (2017) examined the security aspects of Proof of Stake protocols, while Gao et al. (2019) proposed the Trust-Based Practical Byzantine Fault Tolerance (T-PBFT) algorithm to improve the reliability of Byzantine fault-tolerant consensus. Other studies have compared the transaction efficiency of PoS and DPoS (Saad et al., 2021) and analyzed the energy consumption associated with Proof of Work (Saputra & Poetro, 2025). More recent studies have also presented comprehensive reviews of blockchain consensus mechanisms, highlighting their architectural characteristics, performance metrics, and application scenarios (Ge et al., 2022; Shen et al., 2025).

Despite these contributions, existing studies primarily focus on evaluating individual consensus algorithms or comparing only two mechanisms using a limited set of performance indicators, such as energy efficiency, security, or transaction throughput. Consequently, there remains a lack of comprehensive comparative studies that evaluate multiple consensus algorithms using a consistent set of technical parameters. Furthermore, the diversity of evaluation metrics employed across previous studies makes it difficult to perform objective comparisons and identify the most appropriate consensus mechanism for specific blockchain applications.

To address this research gap, this study conducts a comparative analysis of four major blockchain consensus algorithms, namely Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT), using a unified evaluation framework. The comparison is based on several critical technical parameters, including transaction throughput, energy efficiency, communication complexity, transaction finality, network characteristics, and fault tolerance. By employing a standardized evaluation approach, this study aims to provide a systematic understanding of the strengths and limitations of each consensus algorithm, thereby supporting the selection of appropriate consensus mechanisms for different blockchain implementation scenarios.

The primary contribution of this research lies in the development of a comprehensive comparative analysis framework that integrates key technical evaluation parameters into a unified assessment matrix. This framework facilitates the identification of the advantages, limitations, and implementation characteristics of each blockchain consensus algorithm. The findings are expected to serve as a valuable reference for researchers, academics, and blockchain developers in selecting the most suitable consensus mechanism for both permissionless and permissioned blockchain environments.

METHODS

Research Design

This study employed a comparative literature study to analyze the characteristics and efficiency of blockchain consensus algorithms. This approach was selected because the research did not involve system implementation or experimental evaluation. Instead, it focused on reviewing, synthesizing, and comparing findings from previously published scientific studies. Through this approach, the characteristics of different consensus algorithms were systematically evaluated using a unified set of performance parameters, enabling a more objective and comprehensive comparison.

The research data were collected from national and international peer-reviewed journal articles, conference proceedings, and other scholarly publications discussing blockchain consensus mechanisms. Priority was given to publications with high relevance to the research topic published within the last ten years. However, several seminal works that established the theoretical foundation of blockchain technology, such as *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nakamoto, 2008) and *Practical Byzantine Fault Tolerance* (Castro & Liskov, 1999), were also included due to their fundamental contributions to the field.

Research Procedure

The research was conducted through a series of systematic stages, as illustrated in Figure 1.

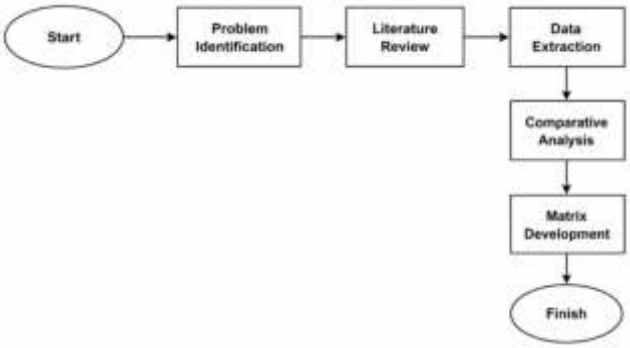

Figure 1. Research Procedure

The research procedure consisted of the following stages.

1. **Problem Identification**
   The first stage involved identifying issues related to the selection of blockchain consensus algorithms. The primary concerns addressed in this study included energy efficiency, transaction throughput, communication complexity, transaction finality, network architecture, and the capability of consensus algorithms to maintain consistency in distributed systems under faulty or malicious node conditions.
2. **Literature Review**
   Relevant scientific publications on blockchain consensus mechanisms were collected from international journals, national journals, conference proceedings, scholarly books, and technical reports. The literature covered the four consensus algorithms analyzed in this study, namely Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT).
3. **Literature Selection**
   The collected publications were screened according to their relevance to the research objectives. Studies that did not discuss blockchain consensus mechanisms or failed to provide technical information regarding consensus algorithm characteristics were excluded from the analysis. This process ensured that all selected references directly supported the objectives of the study.
4. **Data Extraction**
   At this stage, the technical characteristics of each consensus algorithm were identified and systematically extracted from the selected literature. The extracted parameters included:
   a. transaction throughput (Transactions Per Second, TPS);
   b. energy consumption;
   c. transaction finality;
   d. communication complexity;
   e. network characteristics (*permissionless* or *permissioned*);
   f. fault tolerance, referring to the ability of the algorithm to maintain consensus in the presence of faulty or malicious nodes.

   The extracted data were organized into comparative tables to facilitate systematic analysis and interpretation.
5. **Comparative Analysis**
   The extracted data were analyzed using a descriptive-comparative approach. Each consensus algorithm was evaluated based on the predefined technical parameters to identify its strengths and limitations. Furthermore, the findings were interpreted within the context of the Blockchain Trilemma, which explains the inherent trade-offs among security, decentralization, and scalability in blockchain systems.
6. **Conclusion**

The final stage involved synthesizing the comparative analysis results to draw conclusions regarding the performance and implementation characteristics of each consensus algorithm. The conclusions highlight the advantages, limitations, and appropriate application scenarios of the analyzed algorithms, thereby providing guidance for selecting suitable consensus mechanisms in blockchain system development.

Evaluation Parameters

The comparative analysis in this study was conducted using six key evaluation parameters that are widely adopted in the assessment of blockchain consensus algorithms.

Table 1. Evaluation Parameters of Blockchain Consensus Algorithms

Parameter	Description
Throughput	The number of transactions processed per second (TPS).
Energy Efficiency	The amount of energy required to execute the consensus process.
Transaction Finality	The mechanism used to determine the irreversible confirmation of transactions.
Communication Complexity	The amount of communication exchanged among participating nodes during the consensus process.
Network Characteristics	The type of blockchain network supported, namely *permissionless* or *permissioned*.
Fault Tolerance	The capability of the consensus algorithm to maintain system consistency in the presence of faulty or malicious nodes.

These evaluation parameters were selected because they represent the most critical technical aspects commonly used to assess blockchain consensus mechanisms. Employing a standardized set of evaluation criteria enables an objective comparison of the strengths, limitations, and implementation characteristics of each consensus algorithm across different blockchain environments.

RESULTS AND DISCUSSION

Comparison of Blockchain Consensus Algorithm Characteristics

A comparative analysis of blockchain consensus algorithms was conducted to identify the strengths and limitations of each mechanism in supporting blockchain implementation. The analysis focused on six key evaluation parameters: transaction throughput, energy efficiency, transaction finality, network characteristics, fault tolerance, and communication complexity. These parameters were selected because they are the most widely adopted performance indicators in the evaluation of blockchain consensus mechanisms.

Table 2. Comparison of Blockchain Consensus Algorithm Characteristics

Parameter	Proof of Work (PoW)	Proof of Stake (PoS)	Delegated Proof of Stake (DPoS)	Practical Byzantine Fault Tolerance (PBFT)
Throughput	7–15 TPS	1,000–2,000 TPS	2,000–10,000 TPS	>10,000 TPS
Energy Efficiency	Very Low	High	High	Very High
Transaction Finality	Probabilistic	Deterministic	Deterministic	Instant
Network Type	Permissionless	Permissionless	Permissionless / Consortium	Permissioned
Fault Tolerance	<50% computational power	<50% total stake	<50% delegated voting power	<33.3% malicious nodes
Communication Complexity	O(1)	O(N)	O(N)	$O(N^2)$

Table 2 demonstrates that each consensus algorithm possesses distinct characteristics corresponding to its underlying design objectives. Proof of Work (PoW), the earliest consensus mechanism introduced by Bitcoin, is widely recognized for its strong security guarantees achieved through computational mining. However, this mechanism requires intensive computational resources, resulting in substantial energy consumption and relatively low transaction throughput, typically ranging from 7 to 15 transactions per second (TPS).

To overcome the limitations of PoW, Proof of Stake (PoS) replaces computational competition with a staking mechanism, significantly reducing energy consumption while improving transaction processing capacity. In addition to its superior energy efficiency, PoS offers higher throughput than PoW. Nevertheless, the concentration of token ownership among a small number of validators may potentially reduce network decentralization and increase the influence of large stakeholders.

Delegated Proof of Stake (DPoS) further improves blockchain scalability by introducing a representative-based voting mechanism in which token holders elect a limited number of validators (delegates). This approach enables transaction throughput to increase to several thousand transactions per second. However, the relatively small number of validators may reduce decentralization and increase the risk of collusion if the network governance mechanism is not properly maintained.

In contrast, Practical Byzantine Fault Tolerance (PBFT) exhibits characteristics that differ substantially from those of the other consensus algorithms. PBFT is specifically designed for permissioned blockchain environments and provides deterministic transaction finality with extremely high throughput and near-instant transaction confirmation. Nevertheless, its communication complexity grows quadratically ($O(N^2)$), meaning that the number of exchanged messages increases rapidly as the number of participating nodes expands. Consequently, PBFT is more suitable for enterprise or consortium blockchain networks with a relatively small number of nodes rather than large-scale public blockchain systems.

Overall, the comparative analysis indicates that no single consensus algorithm simultaneously optimizes all performance parameters. This finding is consistent with the concept of the Blockchain Trilemma, which states that blockchain systems inevitably face trade-offs among security, decentralization, and scalability. Therefore, the selection of a consensus algorithm should be aligned with the specific requirements and characteristics of the intended blockchain application.

Efficiency Analysis of Blockchain Consensus Algorithms

In addition to comparing the fundamental characteristics of consensus mechanisms, this study evaluates the efficiency of blockchain consensus algorithms using three quantitative performance indicators: transaction throughput, latency, and energy efficiency. These parameters directly reflect the capability of a consensus mechanism to process transactions efficiently while minimizing computational resource consumption.

Table 3. Efficiency Comparison of Blockchain Consensus Algorithms

Consensus Algorithm	Maximum Throughput (TPS)	Average Latency (seconds)	Energy Efficiency
Proof of Work (PoW)	15	140.0	0.2%
Proof of Stake (PoS)	420	4.5	99.8%
Practical Byzantine Fault Tolerance (PBFT)	1200	1.1	99.5%

As presented in Table 3, Proof of Work (PoW) demonstrates the lowest overall efficiency in terms of both transaction processing and energy consumption. Its maximum throughput of approximately 15 TPS is primarily constrained by the computationally intensive mining process, which requires solving cryptographic puzzles with predefined difficulty levels. Although this mechanism provides robust network security, it significantly increases validation time and results in excessive energy consumption, yielding an energy efficiency of only 0.2%.

Compared with PoW, Proof of Stake (PoS) exhibits substantially improved performance. By eliminating computational mining, PoS increases transaction throughput to approximately 420 TPS while reducing the average transaction latency to 4.5 seconds. Moreover, the staking mechanism dramatically decreases energy

consumption, achieving an estimated energy efficiency of 99.8%. These characteristics make PoS one of the most widely adopted consensus mechanisms in modern blockchain platforms because it provides a balanced trade-off among energy efficiency, security, and scalability.

Among the evaluated algorithms, Practical Byzantine Fault Tolerance (PBFT) achieves the highest transaction processing performance. PBFT reaches a throughput of approximately 1,200 TPS with an average latency of only 1.1 seconds, enabling near-instant transaction confirmation. Its energy efficiency is also remarkably high because consensus is achieved through message exchange rather than computational mining. However, these advantages are primarily observed in blockchain networks with a limited number of participating nodes, since communication overhead increases significantly as network size grows.

The comparative analysis further indicates that improvements in throughput are generally accompanied by lower latency and higher energy efficiency, particularly in PoS and PBFT. However, enhanced transaction performance does not necessarily translate into better network scalability. For example, although PBFT provides excellent throughput, its $O(N^2)$ communication complexity causes communication overhead to increase rapidly with network size. Conversely, PoW exhibits relatively simple communication complexity but sacrifices transaction speed and energy efficiency to achieve higher levels of security and decentralization.

Overall, the results confirm that no consensus algorithm consistently outperforms the others across all evaluation criteria. Proof of Work remains appropriate for public blockchain applications that prioritize security and decentralization. Proof of Stake offers a balanced compromise among security, energy efficiency, and scalability, making it suitable for a wide range of contemporary blockchain applications. Meanwhile, Practical Byzantine Fault Tolerance is particularly well suited for private and consortium blockchain environments that require high transaction throughput, deterministic finality, and a relatively small number of participating nodes.

Scalability and Security Analysis of Blockchain Consensus Algorithms

In addition to comparing the general characteristics and operational efficiency of blockchain consensus mechanisms, this study further examines the scalability and security aspects of consensus algorithms. These two aspects are fundamental to blockchain system design because they directly influence the network's ability to maintain data consistency as the number of participating nodes increases and to withstand attacks from malicious or faulty (Byzantine) nodes. The analysis focuses on Practical Byzantine Fault Tolerance (PBFT) and Proof of Work (PoW), as these consensus mechanisms employ fundamentally different approaches to achieving network security.

A. Scalability Analysis of Practical Byzantine Fault Tolerance (PBFT)

Practical Byzantine Fault Tolerance (PBFT) employs a message-passing consensus protocol consisting of three sequential phases: pre-prepare, prepare, and commit. This protocol ensures that all participating nodes reach a deterministic agreement before a transaction is considered valid. However, as the number of participating nodes increases, the volume of exchanged messages also grows significantly, resulting in quadratic communication complexity ($O(N^2)$).

To evaluate the scalability of PBFT, a simulation was conducted to examine the relationship between the number of faulty nodes and the minimum number of participating nodes required to preserve consensus. Furthermore, the simulation estimated the communication overhead generated during each consensus round.

Table 4. Scalability Analysis of the PBFT Consensus Algorithm

Number of Faulty Nodes (f)	Minimum Number of Nodes (N)	Total Messages per Consensus Round	Scalability Level
1	4	24	Very High
2	7	84	High
3	10	180	Moderate
4	13	312	Low
5	16	480	Very Low

Table 4 indicates that the minimum number of participating nodes required to maintain consensus increases linearly with the number of faulty nodes. However, the communication overhead grows considerably faster because the total number of exchanged messages follows a quadratic pattern. For example, when only one faulty node is present, the consensus process requires 24 messages, whereas the presence of five faulty nodes increases the communication overhead to 480 messages.

These findings demonstrate that PBFT is highly efficient in blockchain networks with a relatively small number of participating nodes, such as enterprise or consortium blockchain environments. Conversely, when the network consists of hundreds or thousands of nodes, the communication overhead increases substantially, leading to performance degradation. Consequently, PBFT is better suited for permissioned blockchain systems than for large-scale public blockchain networks.

B. Security Analysis of Proof of Work (PoW)

Unlike PBFT, the security of Proof of Work (PoW) is not achieved through message exchange but through computational competition among network participants. The security of PoW depends on the probability that an attacker can generate a blockchain that surpasses the legitimate chain maintained by honest nodes.

In this study, a security simulation was performed under the assumption that an attacker controls 30% of the total computational power, while the remaining 70% belongs to honest participants. The analysis evaluates how the probability of a successful attack changes as the number of confirmation blocks required before transaction finality increases.

Table 5. Security Analysis of the PoW Consensus Algorithm

Confirmation Blocks	Probability of Successful Attack	Security Level
0	100.00%	Highly Vulnerable
1	42.85%	High Risk
2	21.15%	Moderate Risk
3	10.82%	Reasonably Secure
4	5.64%	Secure
5	2.64%	Highly Secure

As shown in Table 5, increasing the number of confirmation blocks significantly reduces the probability of a successful double-spending attack. When transactions are accepted without waiting for block confirmation ($z = 0$), the probability of a successful attack reaches 100%. However, after five confirmation blocks, the attack probability decreases to approximately 2.64%.

These results reveal an inherent trade-off between transaction security and confirmation time. Waiting for additional confirmation blocks substantially improves transaction security but simultaneously increases transaction latency. Consequently, although PoW provides a high level of security in open blockchain environments, it generally exhibits longer confirmation times than alternative consensus mechanisms.

Overall, the simulation results indicate that PBFT outperforms PoW in terms of consensus speed and transaction finality, whereas PoW provides superior security for permissionless blockchain networks through its computational proof mechanism. These contrasting characteristics highlight that the selection of a consensus algorithm should be based on the intended blockchain architecture, network scale, and security requirements.

Implications for Consensus Algorithm Selection

The comparative analysis demonstrates that each blockchain consensus algorithm possesses distinct characteristics, and no single consensus mechanism consistently achieves the best performance across all evaluation criteria. Therefore, selecting an appropriate consensus algorithm should be guided by the intended application, network architecture, operational requirements, and organizational objectives.

For permissionless blockchain environments, security and decentralization remain the primary design priorities because any participant may join the network without requiring authorization from a central

authority. Under these conditions, Proof of Work (PoW) continues to provide robust network security through computational mining, despite its high energy consumption and relatively low transaction throughput. In contrast, Proof of Stake (PoS) offers a more balanced trade-off among security, energy efficiency, and scalability, making it a preferred consensus mechanism for many modern blockchain platforms that require sustainable operation and improved transaction capacity.

Meanwhile, Delegated Proof of Stake (DPoS) represents an appropriate solution for applications demanding high transaction throughput and rapid confirmation times. By limiting block validation to elected delegates, DPoS significantly enhances network performance. However, this approach also reduces decentralization compared with PoW and PoS, making it more suitable for blockchain networks with clearly defined governance structures.

Unlike the previous mechanisms, Practical Byzantine Fault Tolerance (PBFT) is particularly well suited for permissioned blockchain environments, including enterprise information systems, digital government services, healthcare platforms, and banking applications. In these environments, the relatively small number of participating nodes minimizes communication overhead, allowing PBFT to achieve deterministic consensus with near-instant transaction finality. Consequently, PBFT is highly appropriate for applications requiring real-time data consistency and rapid transaction confirmation.

The findings of this study further reinforce the concept of the Blockchain Trilemma, which describes the inherent trade-offs among security, decentralization, and scalability. Proof of Work primarily optimizes security and decentralization but sacrifices scalability and energy efficiency. Conversely, PBFT provides exceptional scalability and transaction performance within permissioned environments while limiting decentralization due to its dependence on a restricted set of participating nodes. Proof of Stake and Delegated Proof of Stake occupy an intermediate position by offering a more balanced compromise among energy efficiency, security, scalability, and transaction throughput.

Based on the comparative analysis, it can be concluded that there is no universally optimal consensus algorithm for all blockchain applications. Instead, the selection of an appropriate consensus mechanism should consider multiple factors, including the expected level of security, network size, transaction throughput requirements, governance model, energy efficiency, and the operational characteristics of the target blockchain environment. Consequently, choosing an appropriate consensus algorithm represents a strategic architectural decision that directly influences the performance, scalability, and long-term sustainability of blockchain-based systems.

CONCLUSION

This study comparatively analyzed four major blockchain consensus algorithms—Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT)—using key evaluation parameters, including transaction throughput, energy efficiency, transaction finality, communication complexity, network characteristics, and fault tolerance. The results indicate that no single consensus algorithm outperforms the others across all evaluation criteria. PoW provides strong security and decentralization at the expense of high energy consumption and low throughput, whereas PoS offers a balanced trade-off among energy efficiency, security, and scalability. DPoS enhances transaction processing performance through delegated validators but reduces decentralization, while PBFT achieves high throughput and deterministic transaction finality, making it more suitable for permissioned blockchain environments with a limited number of participating nodes. This study contributes a comparative evaluation framework that supports the systematic selection of blockchain consensus mechanisms based on application requirements. Nevertheless, the findings are limited by the use of a comparative literature approach without experimental validation. Therefore, future research should include empirical performance evaluations using blockchain platforms such as Hyperledger Fabric, Ethereum, or EOSIO to validate and extend the proposed comparative framework.

REFERENCES

Castro, M., & Liskov, B. (1999). *Practical Byzantine Fault Tolerance*. Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI), 173–186.

Feng, W. (2025). A comprehensive survey on blockchain technology: Consensus algorithms, data storage mechanisms, and architectures. *Applied and Computational Engineering*. https://doi.org/10.54254/2755-2721/2025

Gao, S., Yu, T., Zhu, J., & Cai, W. (2019). T-PBFT: An EigenTrust-Based Practical Byzantine Fault Tolerance Consensus Algorithm. *Future Generation Computer Systems, 94*, 111–123. https://doi.org/10.1016/j.future.2018.11.041

Ge, Y., Zhang, Y., Wang, X., & Liu, Z. (2022). Survey of consensus algorithms for Proof of Stake blockchain. *Security and Communication Networks*, 2022, 1–18. https://doi.org/10.1155/2022/2812526

Handoko, R. M., Ahmad Trisna, B. A., Pratama, R. D., & Parhusip, J. (2024). Implementasi blockchain untuk keamanan sistem pembayaran digital dan optimasi transaksi keuangan. *Teknik: Jurnal Ilmu Teknik dan Informatika, 4*(2), 64–74.

Li, W., Andreina, S., Bohli, J. M., & Karame, G. (2017). Securing Proof-of-Stake blockchain protocols. In *Lecture Notes in Computer Science* (Vol. 10436, pp. 297–315). Springer. https://doi.org/10.1007/978-3-319-67816-0_17

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

Saad, S. M. S., Radzi, R. Z. R. M., & Othman, S. H. (2021). Comparative analysis of the blockchain consensus algorithm between Proof of Stake and Delegated Proof of Stake. *Proceedings of the 2021 International Conference on Data Science and Its Applications (ICoDSA)*, 175–180. https://doi.org/10.1109/ICoDSA53588.2021.9617549

Saia, J., & Young, M. (2017). *Proof of Work Without All the Work*. arXiv. https://arxiv.org/abs/1708.01285

Saputra, W. I., & Poetro, B. S. W. (2025). Prediksi konsumsi energi menggunakan regresi linier dan multilayer perceptron pada algoritma konsensus Proof of Work (PoW). *Jurnal Rekayasa Sistem Informasi dan Teknologi, 3*(1), 183–197.

Shen, Z., Qu, Q., & Chen, X. B. (2025). Blockchain consensus mechanisms: A comprehensive review and performance analysis framework. *Electronics, 14*(17), 3567. https://doi.org/10.3390/electronics14173567

Wikarsa, L., Suwanto, T., & Lengkey, C. (2022). Implementasi algoritma konsensus Proof-of-Work dalam blockchain terhadap rekam medis. *Jurnal Pekommas, 7*(1), 41–52. https://doi.org/10.56873/jpkm.v7i1.4403

Yulianti, I., Ardiansyah, R., Pusadan, M. Y., Amriana, & Lamasitudju, C. (2025). Evaluasi performa Proof of Work dan Proof of Stake melalui uji stres beban tinggi blockchain. *Jurnal Algoritma, 22*(2), 432–443.